AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A method for tracing content in a highly distributed system, comprising:

receiving content associated with a content owner;

decrypting the received content;

determining a self-identifier that uniquely identifies an entity decrypting the content;

modifying the decrypted content by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier;

encrypting the modified content;

wrapping the encrypted modified content together with the self-identifier using an access key;

and

providing a set of information to the content owner, wherein the set of information enables the content owner to trace the content in the highly distributed system.

2. (Previously Presented) The method of claim 1, wherein decrypting the received content further comprises:

obtaining a different access key out-of-band, wherein the different access key is uniquely associated with the entity decrypting the content and a sender of the content; and

employing the different access key to unwrap the received content before decrypting the received content.

3. (Previously Presented) The method of claim 1, wherein the fingerprint or watermark is further generated based on another self-identifier that uniquely identifies a downstream market recipient of the content.

4. (Previously Presented) The method of claim 1, wherein the self-identifier is digitally signed by an encryption key associated with the entity decrypting the content.

5. (Previously Presented) The method of claim 1, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted.

6. (Previously Presented) The method of claim 1, wherein the set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the entity decrypting the content.

7. (Previously Presented) The method of claim 1, further comprising:

providing the wrapped encrypted modified content and self-identifier to a downstream market recipient;

decrypting, by the downstream market recipient, the received modified content;

further modifying the decrypted modified content by embedding another fingerprint or watermark into the modified content, wherein the other fingerprint or watermark is generated in part from another self-identifier that uniquely identifies the downstream market recipient that decrypts the modified content;

encrypting the further modified content; and

wrapping the encrypted further modified content together with the self-identifier that uniquely identifies the entity decrypting the content and the self-identifier that uniquely identifies the downstream market recipient.

8. (Previously Presented) The method of claim 1, wherein determining the access key further comprises receiving the access key employing an out-of-band mechanism.

9. (Previously Presented) The method of claim 1, wherein wrapping the encrypted modified content further comprises digitally signing the encrypted modified content.

10. (Previously Presented) The method of claim 1, wherein the access key employs a public key infrastructure.

11. (Original) The method of claim 1, wherein the content is at least one of a subscription television, movies, interactive video games, video conferencing, audio, still images, text, graphics.

12. (Currently Amended) A security device for tracing content in a highly distributed system, comprising:

a receiver configured to receive and decrypt encrypted content associated with a content owner;

a fingerprinter-watermarker configured to perform actions including:

determining a self-identifier that uniquely identifies ~~a recipient of~~ the security device decrypting the content;

generating a fingerprint, in part, from the self-identifier; and

watermarking the content employing the fingerprint; and

a forensics interface configured to send information associated with the watermarked content to the content owner.

13. (Previously Presented) The security device of Claim 12, further comprising:

a key wrap, coupled to the fingerprinter-watermarker, that is configured to perform actions, including:

receiving an access key associated with the recipient of the content; and

wrapping the content together with the self-identifier employing the access key.

14. (Original) The security device of claim 13, wherein the access key is received employing an out-of-band mechanism.

15. (Original) The security device of claim 12, wherein the recipient is at least one of an aggregator, a service operator, and a user.

16. (Original) The security device of claim 12, wherein the information associated with the watermarked content comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the recipient of the content.

17. (Original) The security device of claim 12, further comprising:

a data store configured to store decrypted content; and

a fingerprinted-watermarked content data store configured to store encrypted content.

18. (Previously Presented) A network device for managing content in a highly distributed system, comprising:

a transceiver that is arranged to receive and to send content to another network device; and

at least one processor that is configured to execute program code to perform actions, including:

receiving a first wrapper of content from a first market participant sent to a second market participant that is associated with the network device, the wrapper including encrypted content, a first identifier that uniquely identifies the first market participant, and a content key, wherein the encrypted content, content key, and unique first identifier are together encrypted into the first wrapper using an access key associated with the network device;

decrypting the first wrapper using the access key;

decrypting the encrypted content using the decrypted content key;

generating at least one of a fingerprint or a watermark that uniquely identifies the second market participant;

marking the decrypted content by embedding the fingerprint or watermark into the decrypted content;

encrypting the marked content using the content key;

generating a second wrapper that wraps together the content key, the encrypted marked content, the first unique identifier, and a second unique identifier that uniquely identifies the second market participant, using an access key associated with a third market participant; and

transmitting the second wrapper to the third market participant.

19. (Previously Presented) The network device of claim 18, wherein the second unique identifier further includes a time stamp that further indicates when the second wrapper is created.

20. (Previously Presented) An apparatus for tracing content in a highly distributed system, comprising:

a means for receiving content associated with a content owner;

a decryption means for decrypting the received content;

means for determining an identifier that uniquely identifies the entity decrypting the content;

means for modifying the decrypted content by embedding at least one of a fingerprint or watermark generated from the unique identifier into the decrypted content;

means for wrapping the modified content;

a means for determining a set of information associated with the decryption of the content; and

a means for providing the set of information to the content owner.